

Appl. No. 09/693,713
Amdt. dated September 13, 2004
Reply to Office Action of May 12, 2004

PATENT

Amendments to the Drawings:

The attached sheet of drawings includes the addition of Figs. 1A, 1B, and 2A - 2D.

Attachment: Appended Sheets

REMARKS/ARGUMENTS

Claims 1 - 30 and 34 - 37 are pending. Claims 31 - 33 have been canceled without prejudice or disclaimer.

An informality was raised in connection with the specification. Two headings titled BACKGROUND OF THE INVENTION were identified on page 1.

The drawings were objected to for not showing certain elements described in the specification.

Claims 1-6, 13-20, 27-29, 31, and 32 are rejected under 35 U.S.C. 102(a) as being anticipated by Schneier et al., U.S. Patent No. 5,956,404.

Claims 7-12, 21-26, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al., U.S. Patent No. 5,978,475, in view of Schneier et al., U.S. Patent No. 5,956,404.

Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al., U.S. Patent No. 5,956,404 in view of Schneier et al., U.S. Patent No. 5,978,475.

Informality in the Specification

Two headings titled BACKGROUND OF THE INVENTION were identified on page 1. An appropriate correction has been made.

Objection to the Drawings

The drawings were objected to for not showing certain elements described in the specification. In response, Figs. 1A, 1B, and 2A - 2D have been added along with corresponding amendments to the specification. As will be discussed, no new matter has been added by these additional figures.

As to Fig. 1A, the figure shows the addition of a signature log management apparatus 9. This is a variation of the embodiment shown in Fig. 1, and is described beginning on page 16, line 24. Fig. 1A shows that "the signature log management apparatus 9 may be created on the same computer as that on which the digital signature verifier side apparatus 5 resides." *Specification, page 17, lines 11 - 13.* The specification has been amended to add a brief description of Fig. 1A, and to make reference to Fig. 1A as appropriate. No new matter has been

introduced by the addition of Fig. 1A since the figure merely shows that which was described in the specification as originally filed.

As to Fig. 1B, the figure shows the addition a timestamp issuing apparatus 8. The figure shows a configuration of the system wherein "a timestamp issuing apparatus 8, ... is added to a system according to the first embodiment shown in Fig. 1." *Specification, page 28, lines 20 - 22*. The specification has been amended to add a brief description of Fig. 1B, and to make reference to Fig. 1B as appropriate. No new matter has been introduced by the addition of Fig. 1B since the figure merely shows that which was described in the specification as originally filed.

As to Fig. 2A, this figure shows the schematic diagram of Fig. 2 as it applies to the digital signer side apparatus 1, as described in the specification beginning on page 7, line 25. Appropriate references to Fig. 2A have been made in the specification. Accordingly, no new matter has been added since the appended figure merely shows that which has already been disclosed in the specification as originally filed.

As to Fig. 2B, this figure shows the schematic diagram of Fig. 2 as it applies to the purchaser side apparatus 3, as described in the specification beginning on page 8, line 4. Appropriate references to Fig. 2B have been made in the specification. Accordingly, no new matter has been added since the appended figure merely shows that which has already been disclosed in the specification as originally filed.

As to Fig. 2C, this figure shows the schematic diagram of Fig. 2 as it applies to the digital signature verifier side apparatus 5, as described in the specification beginning on page 8, line 11. Appropriate references to Fig. 2C have been made in the specification. Accordingly, no new matter has been added since the appended figure merely shows that which has already been disclosed in the specification as originally filed.

As to Fig. 2D, this figure shows the schematic diagram of Fig. 2 as it applies to the timestamp issuing apparatus 8, as described in the specification beginning on page 28, line 25. Appropriate references to Fig. 2D have been made in the specification. Accordingly, no new matter has been added since the appended figure merely shows that which has already been disclosed in the specification as originally filed.

Section 102 Rejection

The '404 reference discloses a signature generation method that uses past signature information. Kindly see for example, column 6, lines 65 and following. However, the method of the '404 reference differs from the present invention in the following respects:

The present invention relates to a system that determines whether a message having a digital signature is authentic or not based on information registered in a log list. More specifically, the digital signatures are registered in the log list. The digital signatures registered in the log list are used to produce the next digital. With the method of the present invention, forgery remains difficult even if the forger gained access to the secret key (a.k.a., private key) because of the additional reliance of the log list when generating a digital signature.

By contrast, the '404 reference. relates to producing an audit trail and incorporating the audit trail into the padding space of the signature data. *Col. 3, lines 61 - 64.* The '404 reference does not disclose any detail about a log list, although there is mention of "a chain" made in col. 7, line 18. However, data is appended to the chain before generating a signature. *Col. 7, lines 20 and following.* Consequently, the chain does not contain signature data as in the present invention.

Moreover, although the '404 reference describes using a previous signature as a method for leaving an audit trail (see col. 6, line 65 to col. 7, line 15), the reference simply discloses "The token stores the last signature it signed, 327. *Col. 7, lines 2 - 3.* This does not disclose the present invention of managing the signatures as part of a log list. Furthermore, the reference does not disclose how to verify the audit trail using previous signatures.

The claims have been amended according to the foregoing remarks.

Appl. No. 09/693,713
Amdt. dated September 13, 2004
Reply to Office Action of May 12, 2004

PATENT

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "George B. F. Yee", with a stylized flourish at the end.

George B. F. Yee
Reg. No. 37,478

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
Attachments
GBFY
60230241 v1